REMARKS

Claims 71-80 remain pending. The rejections set forth in the Office Action are respectfully traversed below.

Rejections under 35 U.S.C. §103:

Claims 71 - 80 were rejected under 35 U.S.C. §103 over **Choudhury et al.** (USP 5,509,074) in view of **Butter et al.** (USP 5,381,480) and **McCarty** (USP 5,666,411). It is submitted that nothing in the cited prior art, either alone or in combination, teaches or suggests all the features recited in the present claimed invention.

First, the Office action stated that **Choudhury** does not specifically disclose the re-encrypting of decrypted data using a second secret key, nor the handling of storing, copying, and transferring of the re-encrypted data and not the decrypted data.

Moreover, as mentioned before, **Butter** does not disclose or provide motivation directed to achieving data copyright management, and especially not by restricting storage, copying and transferring operations to only re-encrypted data and not decrypted data. To one of ordinary skill in the art, **Butter** does not limit storage or copying of copyrighted data. According to the disclosures of **Butter**, any user (authorized or not) can freely store or copy decrypted data. This is contrary to and **teaches away** from the data copyright protection of the present claimed invention. Indeed, prior rejections relying on **Choudhury** and **Butter** appear to have been distinguished for these reasons.

In addition, the further reference to **McCarty** in the current Office Action does not remedy the deficiencies in the primary references to **Choudhury** and **Butter**. **McCarty** is directed to "customization" of computer software for use on a user's computer. In order to protect mass marketed software, **McCarty** "customizes" the purchased software by re-enchipering the software programs using a second cipher key unique to the user's system (and different from the first cipher key used for the mass marketing of the software) *prior to first use* of the software on the user's system (*see, e.g.*, the Abstract of **McCarty**). The requisite user customization must take place before the protected software program is *run or executed* on the user's computer (column 7, lines 7-19). In providing such customization, **McCarty** emphasizes that his invention "deciphers and enciphers as a single ***indivisible*** operation"(column 5, lines 9-20). According to **McCarty,** "since intermediate results are kept within the crypto microprocessor chip, plain text cannot be accessed by the user." Therefore, decrypted (dechipered) data **cannot be displayed or edited** as recited in the present claimed invention. For at least these reasons, the present claimed invention patentably distinguishes over the prior art.

One skilled in the art would not modify **Choudhury** nor **Butter** to achieve the present claimed data copyright management method since the customization disclosures of **McCarty** expressly prohibit display or editing of the software being re-enchiphered. This is not a trivial difference since the present claimed invention is directed to providing a robust copyright management method in systems wherein copyrighted data is displayed or edited. In contrast to the present claimed invention, the cited prior art do not address the copyright problems that are manifest

in maintaining copyright protection against unauthorized secondary usage or new secondary copyrights associated with copyrighted digital content that is displayed or edited. For at least these further reasons, the present claimed invention patentably distinguishes over the prior art.

Double Patenting:

Claims 71 and 72 were rejected under the judicially created doctrine of obviousness-type double patenting over claim 1 of U.S. Patent No. 6,128,605. The Office Action asserted that it would have been obvious to modify claim 1 of the '605 patent by removing the elements of that claim that makes it an apparatus in order to result in the method claims 71 and 72 of the present application "since both claims actually perform the same function." This is incorrect. Even if it was obvious (and it is not) to simply remove the structural elements of '605 patent claim 1, claim 1 of the '605 patent does *not* recite the *same* function as the present claims 71 and 72. For instance, the '605 patent claim 1 recites re-encrypting a previously decrypted second amount of the encrypted input data, different from the first amount of the encrypted input data, at the same time as the decryption of the first amount, to produce the re-encrypted data. This feature is required in '605 patent claim 1 and cannot be deemed "not needed" as alleged in the Office Action. For at least these reasons, the double patenting rejection should be withdrawn.

Summary:

It is believed that the claims, as amended, contain patentable subject matter, and are now in condition for allowance. Should the Examiner deem that any further action by Applicants would be

desirable to place the application in better condition for allowance, the Examiner is encouraged to telephone Applicant's undersigned attorney.

Attached herewith is a paper showing the claims, as amended, and entitled "VERSION WITH MARKINGS TO SHOW CHANGES MADE."

A three-month petition for extension of time and the requisite fee is attached. If any other fees are due with respect to this paper, such additional fees may be charged to Deposit Account No. 01-2340.

Respectfully submitted,

ARMSTRONG, WESTERMAN & HATTORI, LLP

John P. Kong
Attorney for Applicant(s)
Registration No. 40,054

Attorney Docket No. **990696A**
1725 K Street, N.W., Suite 1000
Washington, D.C. 20006
Tel: (202) 659-2930
JPK/sdj

Enclosures: Version with Markings to Show Changes Made
Petition for Extension of Time

VERSION WITH MARKINGS TO SHOW CHANGES MADE
U.S. Serial No. 09/476,334

IN THE CLAIMS:

Please amend the claims as follows:

71. (Amended) A data copyright management method [for managing the copyright of data] comprising:

encrypting unencrypted copyrighted data using a first secret-key;

supplying the encrypted data to a primary user;

decrypting the encrypted data using said first secret-key;

displaying the decrypted data;

re-encrypting said decrypted data using a second secret-key; and

handling storing, copying and transferring operations on the copyrighted data using said re-encrypted data and not said decrypted data.

73. (Amended) A data copyright management method, comprising:

encrypting unencrypted copyrighted data using a first secret-key;

supplying the encrypted copyrighted data to a primary user;

decrypting the encrypted copyrighted data using said first secret-key;

displaying the decrypted copyrighted data;

re-encrypting said decrypted copyrighted data using a second secret-key; and

handling storing, copying [or] and transferring operations on the copyrighted data using said re-encrypted data and not the decrypted data,

wherein at least one of said decrypting and re-encrypting steps is carried out using a copyright control program.

74. (Amended) A data copyright management method, comprising:

encrypting unencrypted copyrighted data using a first secret-key;

supplying the encrypted copyrighted data to a primary user;

decrypting the encrypted copyrighted data using said first secret-key;

displaying the decrypted copyrighted data;

re-encrypting said decrypted copyrighted data using a second secret-key;

editing said decrypted copyrighted data to produce unencrypted copyrighted edited data;

encrypting the unencrypted copyrighted edited data using said second secret-key;

handling storing, copying [or] and transferring operations on the copyrighted data using said re-encrypted data and not on the decrypted data; and

handling storing, copying [or] and transferring operations on the copyrighted edited data using said encrypted edited data and not the unencrypted edited data,

wherein at least one of said decrypting and encrypting steps is carried out by a copyright control program.